INTERNET I ELEKTRONSKI TERORIZAM

Prof. dr Dušanka Stojanović
Tehnološki fakultet Banja Luka
Stepe Stepanovića br. 73, Tel. 065/663-998
Doc. dr Vesna Marić
Ekonomski fakultet Banja Luka
Majke Jugovića br. 4, Tel 065/523-018
vesna.mŽinecco.net

Apstrakt: U radu su razmatra organizacioni aspekt zaštite od nedozvoljenih ljudskih aktivnosti sa atributom namjernosti, tj. aktivnosti koje imaju karakter kriminalnih radnji. Kontraverze prava i informacionih tehnologija, kao i praznine nastale ubrzanim razvojem informacionih sistema nužno dovode do stvaranja nove pravne infrastrukture koja obuhvata riješenja problema u komunikacijama, prekograničnim tokovima podataka, konsekvencama ranjivosti informacionih sistema, kao i sve učestaliji atak kompjuterskog kriminala.

Ključne riječi: napad na računarsku mrežu, mehanizmi povećana bezbjednosti, praktična realizacija pojedinih sigurnosnih servisa, autorizacija korisnika, identifikacija i autentifikacija korisnika

Abstract: This paper deals with organization aspect of security against computer crime. The law and information technologies controversies, and legal gaps which information systems accelerate, make a new legal inrastructure and new solution in communications, transborder data flaw and consequences of the information systems volunterable, and computer crime attacks, too.

Key words: network security attacks, security mechanisms, practical inplementation of some securitry services, Authorization, Identification and Authentication

UVOD

Pošiljaoci neželjenih poruka ujedinjuju se sa hakerima. U prošlosti su pisanje virusa i zloupotreba sistema bili vid huliganstva. Tinejdžeri su se dokazivali tako što su pisali viruse koji će zaraziti hiljade računara. Potom su hakeri počeli da se pomjeraju od huliganstva ka lakom kriminalu, da razvijaju programe poput trojanaca, malih vrata i špijunskog softvera i da nadgledaju zaražene računare, uključujući i podatke o bankarskim transakcijama i računima korisnika ukoliko je instaliran bankarski program. Dakle, oni su prestali da se dokazuju i počeli su da iskorišćavaju zaražene računare. To je bio drugi korak. Sada je na djelu treći korak, u kome se pošiljaoci neželjene pošte udružuju u novi tip kompjuterskog podzemlja, i treba ga nazvati pravim imenom - to je kriminal. Problem u tome je što je to ujedno i biznis. Sada su hakeri, pisci virusa, u poslu. Oni dobijaju novac od pošiljalaca komercijalne pošte za razvijanje takvih programa. To znači da oni sada imaju više razloga da pišu složenije programe koji se brzo šire. Strahujemo da će se to završiti elektronskim terorizmom. Sve ukazuje na to da se ide u tom pravcu. Mislite li da

hakeri prave crve koji instaliraju sistem za slanje pošte besplatno samo da bi se igrali? Sasvim nevjerovatno. Ali i dalje ne postoje čvrsti dokazi za to udruživanje.
Softver i računarski programi od same svoje pojave bili su predmet rasprave o načinu zaštite. Kako je rastao njihov udio u razvoju informacione tehnologije, to su i ponuđeni modeli bili raznovrsniji. nastajanjem i narastanjem softverske industrije zaštita se stavlja u prvi plan, posebno radi velikih ulaganja u razvoj.
Sa pojavom elektronskog poslovanja i trgovine softveri dobijaju trostruku ulogu: pojavljuje se kao roba koja je predmet ovog poslovanja i trgovine; on je pretpostavka za njihovo funkcionisanje; i, takođe, ključni faktor efikasnosti. Softver se u e-poslovanju, a pogotovo trgovini pojavljuje kao jedan od tipova "nedodirljive" robe, koja se mrežom direktno dostavlja kupcima(potrošačima, korisnicima). Koliki je njegov značaj vidi se iz podatka da među 10 najposjećenijih prodajnih sajtova polovina se odnosi na softver (ostali su muzika, knjige, čestitke, isl.). I da li ga treba štititi, održati bezbjednim?

1. Zaštita podataka u otvorenoj mreži

Masovnom primjenom računara, stvaranjem računarskih mreža i pojavom digitalnog novca, stvari su se drastično promjenile. Masovna komunikacija i ogromna količina informacija u otvorenim mrežama stvorile su potrebu da se podaci štite, da se dokazuje identitet na mreži, da se autentifikuju korisnici.
Stvaranjem Interneta, intraneta i ekstraneta ovaj trend se nastavio samo još intenzivnijim tempom. Pojam *kriptografija* sa Internetom dobija sasvim drugačije značenje od onoga koje je do tada važilo. Pored očuvanja privatnosti poruka, javljaju se pojmovi kao što je autentifikacija, digitalni potpis, sertifikat itd. Kriptografske metode danas obezbjeđuju sljedeće:

- ✶ Zaštitu tajnosti informacija - sprečavanja otkrivanja sadržaja poruke;
- ✶ Sprečavanje neovlašćene izmjene informacija - obezbjeđuju integritet informacija;
- ✶ Provjeru identiteta pošiljaoca - obezbjeđuju autentičnost informacija.

Zaštita tajnosti informacija je najvažniji element, to je razlog za postojanje kriptografije. Savremeni alati za zaštitu tajnosti mogu se podijeliti u *dvije* grupe i to:

- ✶ Simetrično šifriranje ili šifriranje tajnim ključem i
- ✶ Asimetrično šifriranje ili šifriranje sa javnim i tajnim ključem.

2. Ključ šifarskog sistema

Šifriranje sa tajnim ključem, jeste šifarski sistem kod koga su ključ za šifriranje i ključ za dešifriranje *isti*. Kada pošiljalac šifrira poruku tajnim ključem i pošalje je na naznačenu adresu primalac mora imati isti takav ključ da bi poruku mogao da dešifruje. Tajnost i autentičnost ovog šifarskog sistema zasniva se na tajnosti ključa. Osnovni problem pri ovakom načinu rada je distribucija ključeva i sigurnosti njihovog čuvanja. Veliki problem je u tome što ako jedan pošiljalac poruke mora da kontaktira sa većim brojem različitih osoba onda za svaku osobu mora imati poseban ključ. Sa stanovišta današnjih poslovnih transakcija koje se obavljaju preko Interneta ovaj metod nije najpogodniji, stoga je za potrebe elektronske trgovine i poslovanja preko Interneta razvijen novi metod šifriranja.
Asimetrično šifriranje ili sistem šifriranja javnim i tajnim ključem je danas dominantan u svim poslovnim transakcijama preko Interneta. U asimetričnom šifarskom sistemu postoje

dva ključa: jedan je za šifrovanje a drugi je za dešifrovanje, iako su različiti ključevi međusobno povezani određenim transakcijama. Iako možda poznajemo jedan od ključeva nismo u mogućnosti da čitamo poruke. Postupak rada sa ovim načinom šifriranja je slijedeći. Kroz određeni softver se generiše *javni* i *tajni* ključ. Tajni ključ se drži u tajnosti dok se javni ključ redovnom poštom dostavlja svima koji treba da Vam šifriraju poruke. Druga osoba koja je dobila javni ključ sa njim šifrira poruke za Vas, ali nije u stanju da bilo koju drugu poruku dešifruje. Samo vlasnik tajnog ključa je u stanju da poruku dešifruje. Ovo dalje znači da se javni ključ može javno distribuirati svima jer sa njim je moguće samo šifriranje. Ova logika je primjenjena za *provjeru autentičnosti pošiljaoca poruke*. Pošiljalac poruke šifruje poruku svojim tajnim ključem i šalje je primaocu. Ovaj kada poruku primi dešifruje je svojim javnim ključem i može biti siguran da je pošiljalac poruke apsolutno autentifikovana osoba jer jedino on ima i zna tajni ključ.

3. Sertifikat autoriteti

Drugo što obezbjeđuje kriptografija je opisani način autentifikacije osobe koja šalje poruku. Isto tako poruka tokom transporta može biti izmjenjena. Da bi se spriječila izmjena poruka primjenjuje se "digitalni potpis" za potvrdu autentičnosti sadržaja poruke a ujedno on garantuje identitet pošiljaoca poruke. Pošiljalac kreira digitalni potpis primjenom određenih algoritama (softvera) na taj način što stvara zapis fiksne dužine ali takav da u potpunosti oslikava sadržaj poruke. Primalac sa druge strane koristi drugi algoritam za verifikovanje provjerava digitalni potpis, otkriva i provjerava da li je sa porukom nešto rađeno. Ukoliko je bilo šta mjenjano u poruci digitalni potpis se neće slagati što je automatski znak da je poruka izmjenjena.
Na kraju ako želite nekom da pošaljete poruku koju treba da šifrirate javnim ključem morate dobiti njegov javni ključ. Ovdje se javlja kao problem što ne možete biti sigurni da je dobijeni javni ključ baš onaj koji vam je potreban. Ova provjera se postiže upotrebom "digitalnog sertifikata". Na Internetu postoje određene kompanije koje se nazivaju "sertifikat autoriteti" koje provjeravaju i utvrđuju nečiji identitet, primjenjujući visoke standarde bezbjednosti. Oni izdaju digitalne sertifikate kojima se serveri i klijenti predstavljaju jedni drugima. Ovakav način rada služi za poslovnu primjenu prilikom plaćanja preko Interneta i za bankarske transakcije koje se obavljaju takođe na Internetu.

4. Sigurnosni mehanizmi

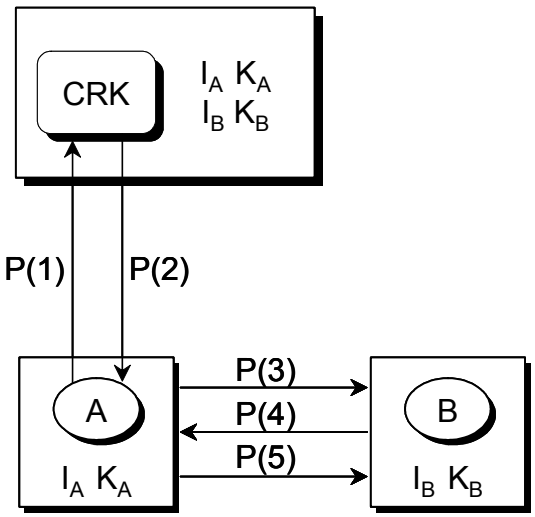
4.1. Sigurnosni protokoli i standardi

Pomenuti simetriči i asimetrični kriptosistemi osnova su za ostvarivanje raznovrsnih sigurnosnih mehanizama. To se područje računarstva danas nalazi u razdoblju intenzivnog razvoja. Međutim, zadnjih dvadesetak godina ustalilo se niz protokola koji su djelimično standardizovani. Mi ćemo u ovom radu opisati neke postupke i mehanizme koji se danas već susreću u svakodnevnoj upotrebi, kao što su: digitalna omotnica (engl. digital envelope), digitalno potpisivanje poruke (engl. digital signature) i sigurnosni zid (engl.firewall) lokalnih mreža.

4.2. Dodjeljivanje ključeva u simetričnim kriptosistemima

Jedno od mogućih rješenja jeste upotreba jednog pouzdanog poslužioca koji će poslužiti za dodjelu ključeva. Svim potencijalnim sudionicima i komunikaciji mora se na pouzdan način (npr. fizičkim raznošenjem) dodijeliti njihov tajni ključ za komunikaciju s tim poslužiocem - centrom za raspodjelu ključeva (engl. key *distribution center*). U

raspodjeljenom sistemu svi učesnici imaju svoj identifikator i pohranjuju samo vlastiti ključ. Dakle, CRK (centar za raspodjelu ključeva) poznaje tajne ključeve svih učesnika. Kada korisnik A želi komunicirati sa korisnikom B (slika 1), on mora od CRK zatražiti tajni ključ koji će važiti samo za tu komunikaciju. Protokol za dodjelu tog ključa[1] sastoji se od 5 poruka P(1) do P(5), kako je to ilustrovano na slici 1[2] . CRK sadrži tablicu svih tajnih ključeva tako da uz identifikatore I_A i I_B koji su javno poznati, može pridružiti tajne ključeve K_A i K_B . Na zahtjev korisnika A koji želi komunicirati sa korisnikom B centar dodjeljuje jednokratni tajni ključ K_{AB}.



Slika 1. Postupak dodijele tajnog ključa

Postupak se izvodi u sljedećim koracima:

✶ Korisnik A generiše neku oznaku zahtjeva Z_A i šalje CRK-u poruku

$$P(1) = (Z_A , I_A, I_B)$$

u jasnom razgovjetnom obliku.

✶ CRK prihvata zahtjev i kreira tajni ključ K_{AB}. Zatim upotrebom tajnog ključ K_{AB} kriptira poruku (K_{AB}, I_A) u kriptovani tekst:

$$C_2 = E((K_{AB}, I_A), K_B)$$

Nakon toga pomoću ključa K_A kriptuje $Z_{A,}$, I_A, K_{AB}, C_2 u poruku P(2):

$$P(2) = E((R_A, I_{A,} , K_{AB} ,C_2), K_A)$$

✶ Jedino korisnik A može dekriptovati poruku P(2). On na osnovu oznaka zahtjeva Z_A i svog identifikatora I_A prepoznaje da je ta poruka odgovor na njegov zahtjev i pohranjuje za dalju upotrebu ključa K_{AB}. Kriptovani tekst C_2 kao cjelinu prenosi u obliku poruke $P(3) = C_2$ učesniku B.

✶ Korisnik B svojim ključem K_B dekriptira C_2 i saznaje I_A , tj. identifikator korisnika koji s njim želi komunicirati kao i ključ K_{AB} . Međutim, korisnik B želi provjeriti posjeduje li A uistinu ključ K_{AB} i zbog toga generiše slučajan broj R_B i kriptuje ga ključem K_{AB} te šalje poruku P(4):

$$P(4) = E (R_B , K_{AB})$$

[1] Predložili su ga R. M. Nedhem i M.D. Schroeer

[2] Broj u zagradi označava redoslijed poruka

✶Korisnik A dekriptira poruku P(4) pomoću K_{AB} i saznaje broj R_B te pomioću unaprijed svim učesnicima poznate funkcije izračunava $N = f(R_B)$, pa kriptuje dobijenu vrijednost ključa K_{AB} i oblikuje poruku P(5):

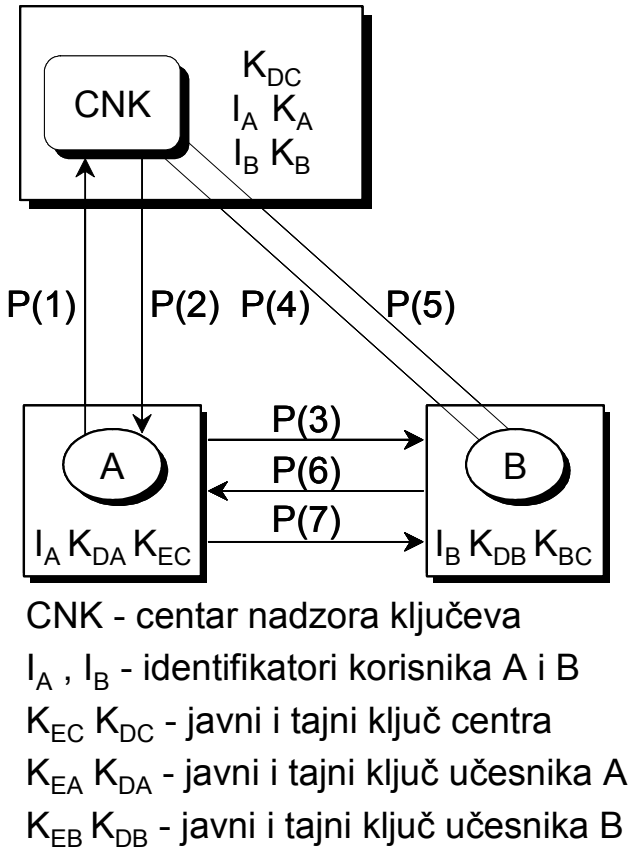
$$P(5) = E((N, K_{AB}).$$

✶ Konačno, korisnik B dekriptuje poruku P(5) i inverznom funkcijom od f (f^{-1}) utvrđuje da li je vraćen broj R_B. Ako je to tačno, uspostavljen je pouzdan informacioni kanal između učesnika A i B.

Može se iz svega uočiti da jedan CRK može postati *preopterećen* u sistemu sa velikim brojem učesnika, a pouzdanost cijelog sistema zavisi o raspoloživosti tog *jedinog poslužioca*. Zbog toga se mogu koristiti i protokoli koji efikasno djeluju u potpuno ili djelimično raspodjeljenom sistemu dodjele ključeva.
Uočen je jedan nedostatak ovog protokola. Npr., ako neki napasnik na komunikaciju snimi poruku P(3) i kriptoanalizom otkrije ključ K_{AB}, on će se u buduće uvijek moći lažno predstavljati korisniku B kao korisnik A i pri tom koristiti taj stari ključ. Taj se problem može riješiti uvođenjem vremenske oznake. Ulogu vremenskih oznaka ilustrovaćemo u sljedećem izlaganju na primjeru raspodjele asimetričnih javnih ključeva.

4.3. Nadzor javnih ključeva u asimetričnom kriptosistemu

Uovom kriptosistemu korisnik A koji želi komunicirati sa korisnikom B upotrebom javnog ključ želi biti siguran da je objavljeni javni ključ pravi ključ korisnika B. Drugim riječima, protokol nadzora javnih ključeva u asimetričnom kriptosistemu ujedno je i *protokol za autentifikaciju učesnika* u komunikaciji. Opisaćemo taj protokol tako da taj opis zajedno s prethodnim opisom raspodjele tajnih ključeva posluži kao ilustracija složenih postupaka kriptovanja, autentifikacije i autorizacije koji se koriste u savremenim sigurnim računarskim sistemima. Opisaćemo sliku 2 i pažljivim praćenjem opisa protokola može se razumjeti mogući način njegovog ostvarivanja.



Slika 2. Nadzor javnih ključeva u asimetričnom sistemu

Svi učesnici u komunikaciji imaju svoj javni ključ K_E i svoj tajni ključ K_D. Oni moraju biti prijavljeni centru za nadzor javnih ključeva (engl. *public-key manager*). U centru se oblikuje tablica javnih ključeva svih potencijalnih učesnika u komunikaciji, a tajni ključevi su pohranjeni samo u čvoru pojedinih korisnika. Centar nadzora ključeva (CNK) takođe ima svoj par ključeva, a svi učesnici u komunikaciji znaju javni ključ centra Slika 2 ilustruje dio sistema u kojem želimo uspostaviti pouzdan informacioni kanal između učesnika A i B (i to na zahtjev korisnika A). CNK sadrži tablicu javnih ključeva i poznaje svoj tajni ključ K_{DC} . Javni ključ centra K_{EC} poznat je svim učesnicima koji su registrovani u centru. Protokol se izvodi slanjem 7 poruka P(1) do P(7), i to na sljedeći način:

✶Korisnik A šalje u centar kriptovanu poruku P(1):

$$P(1) = E((Z_A, T_1 , I_A, I_B),$$

gdje je Z_A oznaka zahtjeva, a T_1 vrijeme postavljanja zahtjeva.

✶ Centar dekriptuje svojim ključem K_{DC} poruku P(1), te pomoću I_A i I_B pronalazi u tablici javnih ključeva K_{EA} i K_{EB}, a pomoću ključa K_{EA} kriptuje poruku P(2):

$$P(2) = E((Z_A, T_1 , K_{EB}), K_{EA})$$

i šalje je korisniku A.

✶ Korisnik A pomoću svog ključa K_{DA} dekriptuje poruku P(2) i na osnovu Z_A i T_1 ustanovljava da je to odgovor na njegovu poruku P(1). On zatim generiše slučajni broj R_A i pomoću javnog ključa K_{EB} kriptuje poruku P(3):

$$P(3) = E((I_A , R_A), K_{eb})$$

i šalje je učesniku B.

✶ Korisnik B pomoću svog tajnog ključ K_{DB} dekriptuje poruku P(3) i saznaje da učesnik A želi s njim komunicirati. On pomoću javnog ključ centra kriptuje poruku P(4):

$$P(4) = E((Z_B, T_2, I_A, I_B), K_{EC})$$

kojom javlja svoju oznaku zahtjeva Z_B i vrijeme zahtjeva T_2 .

✶ Centar svojim tajnim ključem dekriptuje poruku P(4), iz svoje tablice očita K_{EA} i K_{EB} te kriptovanom porukom P(5):

$$P(5) = E((Z_B, T_2, E_{EA}), K_{EB})$$

javlja saučesniku B javni ključ K_{EA}.

✶ Po prijemu poruke P(5) učesnik B svojim tajnim ključem dekriptuje i na osnovu Z_B i T_2 ustanovljava da je to odgovor na njegovu poruku P(4) te prihvata ključ K_{EA} . On sada generiše svoj slučajan broj R_B i kriptuje ga zajedno sa sa slučajnim brojem R_A (koji je od učesnika A dobio u poruci P(3) u poruku P(6):

$$P(6) = E((R_A, R_B), K_{EA})$$

koju šalje učesniku A.

✶ Učesnik A dekriptuje pomoću svog tajnog ključa K_{DA} poruku P(6) i ako je dekriptirani broj R_A jednak broju koji je on poslao, smatra se da je učesnik B autentičan. On potom šalje učesniku B poruku P(7):

$$P(7) = E((R_B, K_{EB}).$$

✶ Konačno, učesnik B dekriptuje poruku P(7) svojim tajnim ključem K_{DB} i ako ustanovi da je vraćeni broj R_B jednak broju odposlatom u poruci P(6), ustanovljava da je A također autentičan.

4.4 Digitalna omotnica i digitalno potpisivanje

Postupak kriptovanja pomoću asimetričnog sistema mnogo je dugotrajniji od simetričnog postupka[3]. Zato je za prenošenje dugačkih poruka asimetrični sistem neprikladan. Zbog toga se dugačke poruke mogu prenositi u tzv. digitalnoj omotnici (engl. *digital envelope*). Nakon što korisnici A i B uspostave pouzdan informacioni kanal i međusobno se autentifikuju (po načinu opisanom u poglavlju 4.3), oni poznaju javne ključeve svojih partnera. Tako korisnik A zna svoj tajni ključ K_{DA} i javni ključ K_{EB}, a korisnik B zna svoj tajni ključ K_{DB} i javni ključ K_{EA}. Postupak slanja informacije u digitalnoj omotnici se odvija na sljedeći način:

✶ Korisnik A bira (npr. pomoću generatora slučajnih brojeva) simetrični ključ K i pomoću njega kriptuje razumljivi tekst informacije koju želi poslati. Time je određen "sadržaj omotnice".

✶ Nakon toga korisnik A svojim tajnim ključem K_{DA} (koji samo on zna) kriptuje simetrični ključ K i priključuje ga sadržaju omotnice. Taj kriptovani ključ čini samu "omotnicu".

✶ Po prijemu "zatvorene omotnice" korisnik B je "otvara" tako da javnim ključem K_{EA} (koji bi on inače koristio za kriptovanje) dekriptuje simetrični ključ K.

✶ Nakon toga korisnik B dobijenim simetričnim ključem K dekriptuje "sadržaj omotnice" i tako raspoznaje informaciju koja mu je poslata.

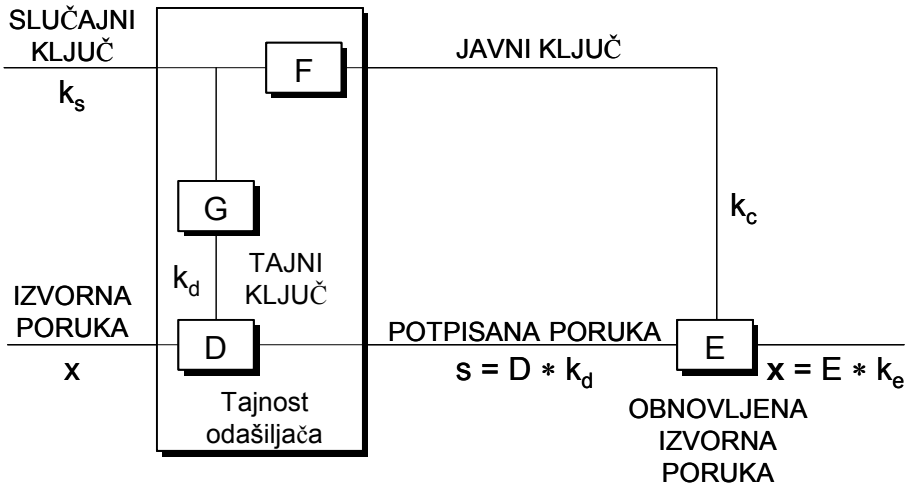
Za utvrđivanje besprekornosti informacije (koja garantuje da se sadržaj nije promjenio tokom prenošenja) može poslužiti tzv. digitalni potpis (engl. *digital signature*). Ako je

[3] Simetrični kriptosistemi omogućuju i do 100 000 puta brže kriptovanje.

informacija primljena u obliku digitalne omotnice, onda bi se umjesto naziva digitalni potpis mogao upotrebiti naziv "digitalni pečat".
Digitalno potpisivanje obavlja se tako da se iz izvornog sadržaja poruke koja se želi potpisati izračunava tzv. sažetak poruke (engl. message digest). Izračunavanje se obavlja tako da se cijela poruka podijeli na skupove bitova jednake dužine i iz tako dobijenog niza brojeva nekom funkcijom (engl. digest function ili hach function) izračunava neki broj određene dužine bitova (npr. 534). Funkcija mora biti takva da postoji mala vjerovatnoća da se za dvije različite poruke dobiju jednaki saželi. Funkcija za izračunavanje sažetka može se smatrati svojevrsnim kriptovanjem poruke.
Protokol po kojem bi se mogla poslati kriptovana i potpisana poruka je prethodni protokol za ostvarivanje digitalne omotnice[4] koji je dopunjen i glasi ovako:

- ✶ Korisnik A bira (npr. pomoću generatora slučajnih brojeva) simetrični ključ K i pomoću njega kriptuje razumljivi tekst informacije koju želi poslati. Time je određen "sadržaj omotnice".
- ✶ Iz izvornog sadržaja informacije korisnik izračunava sažetak S.
- ✶ Nakon toga korisnik A svojim tajnim ključem K_{DA} (koji samo on zna) kriptuje simetrični ključ K i sažetak S. On kriptovani tekst $E((K,S),K_{DA})$ kao "zapečećenu omotnicu" pridodaje "sadržaju omotnice".
- ✶ Po prijemu "zapečećene omotnice" korisnik B je "otvara" tako da javnim ključem K_{EA} otkriva simetrični ključ K i sažetak S.
- ✶ Nakon toga korisnik B dobijenim simetričnim ključem K dekriptuje "sadržaj omotnice" i tako saznaje poslanu mu informaciju.
- ✶ Iz dekriptovanog sadržaja informacije korisnik B izračunava sažetak S i ako su te dvije vrijednosti jednake, smatra primljenu informaciju vjerodostojnom.

Primjena tehnike digitalnog potpisa principjelno je prikazano slikom 3.



Slika 3. Tehnika digitalnog potpisa

[4] Ostvarivanje digitalne omotnice i digitalnog potpisivanja nalazimo u programskom sistemu *Privacy Enbanced Mail* (PEM) korišćenom za unapređivanje elektronske pošte u Internetu.
Drugi program za podržavanje sigurnih komunikacija koji se koristi u Internetu je program Pretty Good Privacy (PGP). Za razliku od PEM sistema on ne koristi DES simetrični kriptosistem već sistem s karticom IDEA. Takođe, proizvođač programa tvrdi da koristi jednu nezaštićenu varijantu RSA asimetričnog kriptosistema.

Objašnjenje uz sliku 3.

Digitalni potpis nije vlastoručni potpis (paraf) na dokumentu u klasičnom smislu, nego kriptovana izvorna poruka, modifikovana time što što se u kriptogram ugrađuje (dodaje) zasebni (obično završni) dio, koji je, kao i sama poruka, kriptovan metodom javnog ključ, tj. asimetričnom šifrom. Sadržaj tog dodatnog dijela može biti određen na različite načine, bilo kojom metodom slučajnog izbora (engl. Random Sampling) dijelova izvorne poruke ili u obliku neke vrste njezinog sažetka (engl. Plaintext Digest).

5. NADZOR I KONTROLA

Naglasimo da i pored zaštite pomenute u prethodnom izlaganju, korisnici računarskih mreža moraju shvatiti i prihvatiti potrebu strogog nadzora i kontrole svih učesnika u procesu automatske obrade, a posebno neposrednih izvršilaca. Nadzor i kontrola imaju trostruku funkciju: preventivnu, korektivnu i detektivnu. Kontrola se mora striktno i uniformno sprovoditi svo vrijeme, a preporuka je da se prethodno izvrši precizno i cjelovito razdvajanje dužnosti i odgovornosti, kako bi se obezbjedilo da:
- nijedan pojedinac ne može isključivo biti odgovoran za vitalne funkcije;
- za sprovođenje ilegalne aktivnosti mora biti neophodna saradnja najmanje dva radnika (dobro dizajniran sistem nadzora i kontrole obezbjeđuje brojne tačke na kojima se nedozvoljene aktivnosti mogu otkriti i prije dobro postavljene efikasne zaštite kriptografijom; time je mogućnost za izvršenje kriminalnih radnji značajno redukovano).
Pozitivna svojstva nadzora i kontrole: povećava pažnju zaposlenih, obezbjeđuje poštovanje postupka, daje informaciju o adekvatnosti zaštite, otežava nedozvoljene aktivnosti,blokira nedozvoljene aktivnosti.
Nameće se zaključak da bi svaki sistem zaštite koji ne počiva na dobro osmišljenoj i čvrsto zasnovanoj organizaciji unaprijed bio osuđen na propast. Jer, besmisleno je ulagati sredstva u skupa tehnička rješenja koja smo pomenuli ili rasipati vrijeme i snagu na izgradnji složenih lozinki, ako prethodno nisu regulisane elementarne stvari kao što su: disciplina, odgovornost, evidentiranje izvršenih poslova, nekontrolisana distribucija listinga, uništavanje nevažeće dokumentacije i sl. Ni kripto uređaji, ni dovoljno pouzdane lozinke koji mogu zaštititi informacioni sistem u ambijentu u kojem se ne zna ko, šta i kako treba , može i mora da radi, ne pomažu cjelovito rješenje zaštite.

ZAKLJUČAK

Kada se govori o profesionalnoj kriptografiji moraju se jasno razgraničiti oblasti primjene:
- kriptozaštita za specijalne korisnike (vojska, policija i sl.) i
- kriptozaštita za komercijalnu upotrebu (tj. za kompanije koje žele da svoje poslove komunikacije ili arhiviranja podataka zaštite). U članku smo se bazirali na kriptografiju koja se koristi u poslovne i administrativne svrhe.
Profesionalna kriptozaštita za komercijalne svrhe se može realizovati na dva načina: hardverski i softverski. *Hardverska* realizovana kriptozaštita se odnosi na posebne uređaje koji vrše kriptovanje, uglavnom digitalnih podataka. Jedna varijanta je da se kriptovanje vrši u procesoru opšte namjene, a na osnovu određenog softvera koji se drži u nekoj od

memorija. Druga varijanta je da se kompletan algoritam realizuje hardverski na posebnom čipu napravljenom samo za ovu namjenu[5].
Softverska rješenja su znatno jeftinija od hardverskih, ali kod njih se javlja problem bezbjednosti, naročito u pogledu čuvanja i distribucije ključeva (ili šifara ako je to jasnije). Ova rješenja su ipak vrlo prikladna za zaštitu podataka u privatnim komunikacijama ili u komunikacijama između malog broja korisnika, gdje se relativno lako može uspostaviti potreban stepen "bezbjedonosne discipline". Za veće organizacije, velike komunikacione mreže i sl. jedina pouzdana rješenja su ipak hardverska.
Iako je neovlašćeni pristup računaru još uvijek marginalan, relativan, njegove posljedice počinju uznemirivati brojne informatičke kuće, mreže, pojedince... Metode malverzacije su mnogobrojne i često gotovo nezamislive: od krađe do neovlašćenog prisluškivanja na mreži. Novija američka studija pokazuje da se informatički kriminal dešava 40 puta češće od tradicionalno poznatog. Rizici su mnogobrojni. Uprkos tome što su identifikovani slučajevi još uvijek malobrojni (90% informatičkog zločina još uvijek ostaje neotkriveno) moguće je izvršiti tipologiju kriminalnih radnji(dobrovoljna sabotaža, krađa informacija, pronevjera, krivotvorenje i sl) a time i pristupiti boljoj organizaciji bezbijednih informacionih mreža.
Budućnost bezbijednosti mreža prolazi kroz evoluciju tehnologije i razvoja kartica pristupa, posebno što se tiče mikroprocesora koji bi mogli u sebi pohranjivati vrlo osjetljive podatke. Moguće je takođe, zasnovati određenu nadu na moćnim sistemima kriptozaštite a pogotovo digitalnog "potpisa" na javnim mrežama.

LITERATURA

1. Merkle, R.C., *A Certified Digital Signature*, Technical Report No. 1979-1, Information System Library, Stanford Elecronics Laboratories, Stanford, ca., 1980.
2. Merkle, R.C., *Secrety, authentication, and public-key systems,* Technical Report No. 1979-1, Information System Library, Stanford Elecronics Laboratories, Stanford, ca., 1979.
3. Stojanović, D., *Primjena kriptografske zaštite u sigurnom informacijskom sustavu,* doktorska disertacija, ETF Zagreb, 1989.
4. Stojanović, D., *Kompjuterski informatički sistem u funkciji kriptozaštite,* Tehnološki fakultet Banja Luka, 1993.
5. Stojanović, R., *Konceptualni pristup kriptozaštiti informacija,* NTB (NAUKA TEHNIKA BEZBEDNOST), Institut bezbednosti, Beograd, 1998.
6. Stojanović, D., Marić, V., *Bezbjedna mrežna komponenta poslovnih upravljačkih informacionih sistema,* Zbornik radova, Ekonomski fakultet Brčko, 2001. str. 215-222.
7. Stojanović, D., Marić, V., *Zaštita informacionog sistema - INTERNET-a od pristupa neovlašćenih korisnika*, XXVIII Jugoslovenski simpozijum o operativnim istraživanjima (SYMOPIS 2001), Zbornik radova, Beograd, 2001. str. 249-353.

[5] Prvi princip je znatno fleksibilniji što se tiče kasnijih promjena kao i jeftiniji, ali je nešto manje bezbjedan i relativno spor za primjenu na komunikacionim linijama. Drugi princip se smatra znatno bezbjednijim, ali je i skuplji.

8. Stojanović, D., Milić, Lj., *Aspekti zaštite od računarskog kriminala*, XXVII Jugoslovenski simpozijum o operativnim istraživanjima (SYMOPIS 2001), Zbornik radova, Beograd, 2001. str. 253-257.

9. Stojanović, D., Praštalo, R., *Kriptosistem za bazu podataka,* Elektrotehnički fakultet Podgorica, Zbornik radova ETF Podgorica, 1998.

10. Williams, H.C., *A modification of the RSA public-key encryption procedure,* IEEE Trans. Inform. Theory, IT-26, 1988, pp 726-9.